IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Case No. 7:22cr00001**
	:	
JERALD FRANCIS GRAY	:	

UNITED STATES' MEMORANDUM IN RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS

COMES NOW the United States of America, by counsel, and respectfully opposes the motion to suppress filed by the Defendant, Jerald Francis Gray. In short, the Defendant seeks to suppress evidence obtained as a result of a search conducted on his computer pursuant to a warrant. For the reasons explained below, the Government respectfully requests that the motion be denied.

BACKGROUND

A. Factual Background

1. Freenet

This case involves the illicit use of a computer network called Freenet, a peer-to-peer file-sharing network designed to permit users to remain anonymous while exchanging files. Ex. 1 (Aff. of Kathryn Weber) ¶ 6. When a user uploads a file into Freenet, the file is broken into pieces, with each piece stored on the hard drive of another user of the network. Ex. 1 ¶ 9. These pieces are then encrypted. Ex. 1 ¶ 9. A "key"—similar to a password—is then needed in order to be able to collect all of these pieces to put this puzzle back together and access the full file. Ex. 1 ¶¶ 9–11. The user who uploaded the file receives the key, which can then be shared with other users to enable them to download the file. Ex. 1 ¶¶ 9–10, 17–19.

When a user wants to retrieve a particular file from Freenet, the user enters the key associated with the file. Ex. 1 ¶ 10. Freenet then attempts to collect all of the stored encrypted pieces of that file from the user's peers.[1] Ex. 1 ¶ 11. That is, the network will ask each peer if it has pieces of that file stored on its hard drive. Ex. 1 ¶ 11. If a peer has the requested piece, it fulfills that request and provides the piece to the requester. *See United States v. Dickerman*, 954 F.3d 1060, 1063 (8th Cir. 2020). When a peer does not have one of the pertinent pieces, it relays that request to each of *its* peers. Ex. 1 ¶ 11. Requests typically continue to be relayed up to a maximum of eighteen times. Ex. 1 ¶ 12. A particular number of requests (the hops-to-live—or HTL—count) is assigned to each Freenet request. *See* Ex. 3 (Brian N. Levine academic paper), at 3; *United States v. Pobre*, Criminal Action No. 8:19-cr-348-PX, 2022 WL 1136891, at *2 (D. Md. Apr. 15, 2022). The HTL count is something that is knowable to Freenet users as a part of Freenet's normal operation. Ex. 1 ¶ 20.

To put all of this more concretely, if a user is seeking a file that consists of 1000 pieces and that user has ten peers, the user's computer will request approximately 100 pieces from each peer. If one of those ten peers does not have all of the 100 pieces that the original user is seeking, and that peer has ten peers of its own, then that peer's computer will request approximately ten of those 100 pieces from each of *its* peers. This design can help law enforcement determine whether a computer requesting a piece of a file is the original requester or whether that computer is merely relaying that request from the original requester because relayed requests necessarily seek fewer pieces than original requests. Ex. 1 ¶¶ 11, 24. And, because the HTL count of each original request is by default eighteen, without additional modification to how this procedure operates, it would be

[1] "Peers" are other computers using Freenet to which a user's computer is connected. Ex. 1 ¶ 8. Users select for themselves the number of peers with which they wish to connect, although, once they set that number, Freenet selects *which* peers with which a user connects. *United States v. Weyerman*, 2:19-cr-88-PD, at *3 (E.D. Pa. Jan. 3, 2020) (attached as Ex. 2), *aff'd*, No. 21-1896, 2022 WL 1552997 (3d Cir. May 17, 2022).

extremely obvious how to distinguish original requesters from relayers—all requests with an HTL count of 18 would be original requests, while all of those with an HTL count of fewer than 18 would be relayed requests.

In order to help conceal the identity of its users, Freenet randomly assigns an HTL of 17 (instead of 18) to approximately half of the original requesters, with the other half being assigned an HTL of 18. Ex. 1 ¶ 13. This allows Freenet to attempt to conceal the identity of the original requester by blurring the line between original requesters and relayers.

Nevertheless, Freenet's operation is predictable enough that mathematical and computer science techniques have allowed law enforcement to predict whether a particular request is an original request or a relayed request with a high degree of accuracy. Ex. 1 ¶¶ 23–24. Computer scientists from the University of Massachusetts and the Rochester Institute of Technology developed a formula that takes into account publicly available information connected to each Freenet request—specifically, the number of peers a requester has and the number of requests received from the requester—and deduces the probability of whether a request is an original request or a relayed request. Ex. 1 ¶¶ 20, 23–24; Ex. 3, at 5. The mathematical details of the technique are complicated and are described in the attached paper. But the technique is rooted in the relative predictability of Freenet's operation (i.e., that requests are split roughly evenly among each of a requester's peers) and the intuitive idea that an original request will submit a request for a larger number of pieces than will a relayed request, since any relayed request will be further subdivided among each relayer's peers.

The peer-reviewed paper in which this algorithm is described in greater detail has found the algorithm to be highly accurate, with a high true positive rate and a low false positive rate. Ex. 1 ¶ 24; Ex. 3, at 7–8. In fact, the false positive rate (i.e., the frequency with which a relayed request

is wrongly thought to be an original request) has been found to be approximately two percent. *United States v. Sigouin*, 494 F. Supp. 3d 1252, 1268 (S.D. Fla. 2019). Law enforcement has conducted dozens of searches of devices that were flagged by this Freenet algorithm, and the vast majority have yielded evidence of child exploitation. Ex. 1 ¶ 25.

2. The Search Warrant

On two different dates in 2021, a computer assigned an IP address later found to be tied to an Internet account registered in the Defendant's name made three requests via Freenet for pieces of three files known to contain child sexual abuse material. Ex. 1, at 15–18.[2] Based on the algorithm described above and other pertinent information, law enforcement concluded that this computer—the Defendant's computer—was the original requester of these files. Ex. 1 ¶ 26.

Based on the information described above,[3] and other information, Special Agent Kathryn Weber of the Federal Bureau of Investigation sought a search warrant for the Defendant's home, including his electronic devices. On December 3, 2021, United States Magistrate Judge Robert S. Ballou found that Agent Weber's affidavit established probable cause and signed off on a warrant. Ex. 4. Law enforcement than executed that warrant on the Defendant's home and, as a part of that search, located child sexual abuse material on the Defendant's computer.

B. Procedural Background

On January 13, 2022, a grand jury in this District returned a one-count indictment charging the Defendant with possession of child pornography depicting minors under the age of twelve, in

[2] The search warrant affidavit contains two each of paragraphs 29, 30, 31, and 32. For ease of reference, page numbers are used for this citation instead of using paragraph numbers.

[3] As is apparent from the citations, almost all of the previously-described information was in Agent Weber's affidavit. And, as is discussed in greater detail below, the information that was not included only would have bolstered the case for probable cause.

violation of 18 U.S.C. § 2252(a)(4)(B), (b)(2). Indictment (ECF No. 27). The Defendant has now moved to suppress the evidence underlying this charge.

ANALYSIS

It is difficult to discern the exact basis for the Defendant's motion. On the one hand, the Defendant complains that Judge Ballou was not given "an understandable description of the algorithm used in this case" or "a description of how it in fact was used" and thus the Defendant contends that Judge Ballou "was not given enough information to allow him to adequately assess whether the police were acting on probable cause." Def.'s Mot. to Suppress Evid. 4–5 (ECF No. 84). This sounds like an argument that the affidavit contained insufficient information to support a finding of probable cause. On the other hand, the Defendant contends that law enforcement intentionally withheld "key information necessary for the Magistrate to conduct an independent assessment of probable cause." Def.'s Mot. to Suppress Evid. 5. This sounds like an allegation of a *Franks* violation[4] in that law enforcement made an omission that was "designed to mislead . . . the magistrate." *See United States v. Haas*, 986 F.3d 467, 474 (4th Cir. 2021) (internal quotation marks omitted). But an argument that an affidavit was insufficient to support probable cause is not a *Franks* argument. *See id.* at 475 ("[T]he presence (or absence) of probable cause is not the proper subject of a *Franks* hearing."). The Government construes the motion to be making two alternative arguments: (1) that the affidavit failed to establish probable cause and (2) while the affidavit established probable cause, it would not have done so had additional information about the algorithm been included. The Government addresses each argument in turn.

[4] Indeed, one of the few cases that the Defendant cites is *Franks v. Delaware*, 438 U.S. 154 (1978).

A. Probable Cause

"[P]robable cause is a fluid concept . . . turning on the assessment of probabilities in particular factual contexts . . . ." *Illinois v. Gates*, 462 U.S. 213, 232 (1983). "[A] finding of probable cause does not require absolute certainty," *United States v. Gary*, 528 F.3d 324, 327 (4th Cir. 2008), but only "a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. The quantum of proof required is less than a preponderance. *United States v. Gondres-Medrano*, 3 F.4th 708, 714 (4th Cir. 2021). It need only be the case that, in light of the "combined circumstances," suspicion is warranted. *Id.* (internal quotation marks omitted). An evaluation of whether probable cause exists is "a practical, common-sense decision." *Id.* (quoting *Gates*, 462 U.S. at 238).

The Defendant contends that Agent Weber's affidavit could not have supported a finding of probable cause because the affidavit lacked sufficient information about the algorithm that was used to determine whether the Defendant was the original requester of the files containing child sexual abuse material or whether he was merely relaying the request from one of his peers. But this focuses too much on what was not in the affidavit and ignores what *was* in the affidavit. As explained above, Agent Weber's affidavit explained how the Defendant's computer sent three requests for pieces of files containing child sexual abuse material to a law enforcement computer on two separate dates. Even setting aside the implausibility of the idea that the Defendant's computer just happened to relay requests for pieces of files containing child sexual abuse material three separate times on two different dates, Agent Weber's affidavit specifically explained how she was able to determine that it was likely that the Defendant was the original requester of these files. She explained how the algorithm was created and how it was published in a peer-reviewed academic paper. She explained how that paper detailed that the algorithm was extremely accurate

and how law enforcement experience with the algorithm had proven that to be true. And she explained how the algorithm was used in this case to determine that there was a high likelihood (that is, more than "a fair probability") that the Defendant was the original requester of these file pieces, based on the number of file pieces requested by the Defendant's computer, the total number of pieces required to assemble the file, and the number of peers the Defendant had. Agent Weber also offered to make the entire academic paper available to Judge Ballou, Ex. 1 ¶ 24 n.4, and Judge Ballou's determination that a review of that paper was not necessary to find probable cause is entitled to deference, *see United States v. Orozco*, 41 F.4th 403, 407 (4th Cir. 2022).

It is not clear what additional information the Defendant believes the Magistrate should have been provided. And given the power and precision of the algorithm at issue, any additional information about the algorithm could only have served to *bolster* the case for probable cause. It is curious for the Defendant to be arguing that the Magistrate should have been provided with an even more persuasive case for authorizing the warrant. *See United States v. Dunning*, 857 F.3d 342, 347 (6th Cir. 2017) (noting that providing reliability information about the software law enforcement used "would have only strengthened the affidavit"); *United States v. Chiaradio*, 684 F.3d 265, 279–80 (1st Cir.2012) ("It would be wildly illogical to suppress the fruits of a search on the ground that the warrant application omitted statements that, if included, would have *increased* the affidavit's persuasive force.").

Notably missing from the Defendant's motion is a single case—not in the Freenet context or in any other—granting a motion to suppress because a law enforcement agent failed to provide technical information underlying the details provided in the affidavit, despite a myriad of analogous situations. He relies only on a confusing and unsuitable analogy and empty rhetoric. Moreover, as far as the Government is aware, no court has granted a motion to suppress for failure

to disclose sufficient details about law enforcement techniques used to track users on Freenet or any other peer-to-peer file-sharing network. *See, e.g.*, *Dickerman*, 954 F.3d at 1067–69 (Freenet); *Dunning*, 857 F.3d at 347 (eDonkey); *United States v. Schumacher*, 611 F. App'x 337, 340 (6th Cir. 2015) (Gnutella); *Chiaradio*, 684 F.3d at 279–80 (LimeWire); *United States v. Weyerman*, 2:19-cr-88-PD, at *11–13 (E.D. Pa. Jan. 3, 2020) (attached as Ex. 2) (Freenet), *aff'd*, No. 21-1896, 2022 WL 1552997 (3d Cir. May 17, 2022); *Sigouin*, 494 F. Supp. 3d at 1267–68 (unnamed network); Hr'g Tr., at 155, *United States v. Hall*, 1:16-cr-00469 (ECF No. 61) (D. Md. Aug. 30, 2017) (Freenet) (excerpt attached as Ex. 5); Hr'g Tr., at 37–42, *United States v. Hebert*, 2:16-cr-0104-SWS (ECF No. 127) (D. Wyo. Oct. 7, 2016) (Freenet) (excerpt attached as Ex. 6).

Nor is it a novelty that an affidavit will provide conclusions drawn from technical analyses without going into painstaking detail about the technical details. For example, it is common for a search warrant affidavit to state that a particular person has been linked to a location or evidence because of a DNA match without including much detail about the technical analysis that resulted in that match. *See Sigouin*, 494 F. Supp. 3d at 1268.

Because Agent Weber's affidavit was sufficient to support a finding of probable cause and because any additional information about the algorithm used would have only bolstered that finding, the Defendant's motion should be denied.

B. *Franks*

Under *Franks v. Delaware*, 438 U.S. 154 (1978), a defendant may establish a Fourth Amendment violation by establishing both 1) that an affiant to a search warrant intentionally or recklessly omitted facts from the affidavit and 2) that these facts were material. *United States v. Pulley*, 987 F.3d 370, 376 (4th Cir. 2021). To prove the first prong of this analysis—intentionality—a defendant must prove that the affiant "omitted information from the affidavit

'with reckless disregard of whether it would make the affidavit misleading.' " *Id.* (quoting *United States v. Lull*, 824 F.3d 109, 115 (4th Cir. 2016)). Proving "reckless disregard" requires establishing that the particular affiant was "subjectively aware that the . . . omission would create a risk of misleading the reviewing magistrate judge and nevertheless chose to run that risk." *Id.* at 377. This is a high burden "because an affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation." *Id.* at 376–77 (quoting *Lull*, 824 F.3d at 115). Moreover, "because of the presumption of validity with respect to a search-warrant affidavit, conclusory allegations of a defect are insufficient." *Id.* at 377.

The Defendant's failure to identify specific information that was omitted from the affidavit renders his allegation conclusory, "[a]nd conclusory allegations fail." *Haas*, 986 F.3d at 475. This alone is enough to doom the Defendant's *Franks* argument. But, beyond that, the Defendant cannot prove reckless disregard (and thus he cannot prove intentionality) or materiality because, as explained above, the inclusion of any information omitted from the affidavit would only have strengthened the case for probable cause.[5]

C. Good Faith

Even if the Court were to find the affidavit at issue to be defective, the good faith exception should apply. "[E]vidence 'seized in reasonable, good-faith reliance on a search warrant that is subsequently held to be defective' is not subject to suppression, despite the existence of a constitutional violation." *United States v. Brunson*, 968 F.3d 325, 334 (4th Cir. 2020) (quoting

[5] "To obtain a *Franks* hearing, a defendant must make a 'substantial preliminary showing' to overcome the 'presumption of validity with respect to the affidavit supporting the search warrant.' " *Haas*, 986 F.3d at 474 (quoting *United States v. Moody*, 931 F.3d 366, 370 (4th Cir. 2019)). "When a defendant relies on an omission, this heavy burden is even harder to meet." *Id.* Not only has the Defendant failed to meet this heavy burden, but he has also not requested a hearing. The Government agrees that no hearing is necessary here.

United States v. Leon, 468 U.S. 897, 905 (1984)). This good faith exception does not apply in four circumstances:

> (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate wholly abandoned his judicial role . . . ; (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.

United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (quoting *United States v. DeQuasie*, 373 F.3d 509, 519–20 (4th Cir. 2004)).

The Defendant makes no allegation that the affidavit contained false information or that the magistrate was misled in any way. There is no basis to believe that Judge Ballou "wholly abandoned his judicial role." And it strains credulity to argue that this detailed, thirty-six-page affidavit "is so lacking in indicia of probable cause" or "so facially deficient" that no reasonable officer could rely on it. This is particularly so where the only information that the Defendant alleges is missing from the affidavit is information "*supporting* a finding of probable cause." *United States v. Bynum*, 293 F.3d 192, 198–99 (4th Cir. 2002).

CONCLUSION

For all of these reasons, the Government respectfully requests that the Court deny the Defendant's motion to suppress.

Respectfully submitted,

CHRISTOPHER R. KAVANAUGH
United States Attorney

/s/ Jason M. Scheff
Jason M. Scheff
Assistant United States Attorney

New York Bar No. 5188701
United States Attorney's Office
310 First Street, SW, 9th Floor
Roanoke, Virginia 24011
540-857-2250
Jason.Scheff@usdoj.gov

/s/ Matthew M. Miller
Assistant United States Attorney
VA Bar No. 43034
Matthew.Miller2@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on October 6, 2022, I caused to be filed electronically this Memorandum in Response to Defendant's Motion to Suppress with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

s/Jason M. Scheff
Assistant United States Attorney